Doc Code: AP.PRE.REQ

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional): 555255-012130

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)]

on November 18, 2005

Signature: Jacqueline M. O'Brien

Typed or printed name: Jacqueline M. O'Brien

Application Number	Filed
09/594,368	June 15, 2000

First Named Inventor: Herb A. Little

Art Unit	Examiner
2137	Tamara Teslovich

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

- [ ] applicant/inventor.
- [ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)
- [x] attorney or agent of record. Registration number 45,910
- [ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34 _____

Signature

Paul E. Franz
Typed or printed name

(216) 586-1162
Telephone number

November 18, 2005
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

- [x] *Total of 3 forms are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Group Art Unit:	2137	
Examiner:	Tamara Teslovich	
Inventor:	Herb A. Little	
Serial No.:	09/594,368	**REASONS FOR PRE-APPEAL BRIEF CONFERENCE REQUEST**
Filed:	6/15/2000	
For:	Public Key Encryption With Digital Signature Scheme	
Atty. Docket:	555255-012130	

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited today with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1459 on 11/18/2005.

Signature: Jacqueline M. O'Brien

Typed or Printed Name: Jacqueline M. O'Brien

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Claims 1-45 stand finally rejected. In particular, claims 1-10, 16-25 and 31-40 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 5,761,305, issued to Vanstone et al. ("Vanstone"); claims 1, 16 and 31 stand finally rejected under 35 U.S.C. § 102(b) as being anticipated by IBM Technical Bulletin NN9305343 ("IBM Reference"); and claims 11-15, 26-30 and 41-45 stand finally rejected under 35 U.S.C. § 103(a) as being obvious over Vanstone in view of C. Boyd & A. Mathuria, Key Establishment Protocols For Secure

Mobile Communications: A Selective Survey, Australian Confernece On Information Security And Privacy Proceedings, July 13, 1998 ("Boyd").

The rejections of claims 1-45 are now appealed. The Applicant hereby requests review of the final rejection prior to filing an appeal brief for the reasons set forth below. The Applicant submits that the rejections of the independent claims 1, 16 and 31 over Vanstone and the IBM Reference are based on clear errors in fact and thus independent claims 1, 16 and 31, and all claims depending therefrom, are not anticipated by or obvious over the art of record.

I. Vanstone Clearly Does Not Anticipate Claims 1, 16 And 31

Claim 1 reads as follows[1]:

1) A public-key encryption process comprising the steps of:

   a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair; and

   b) signing a digital signature using the ephemeral key pair.

Claim 1 recites that a plaintext message is encrypted into a ciphertext message and in the encrypting step, an ephemeral key pair is produced. That ephemeral key pair is then used in signing a digital signature.

The Examiner maintains that the Vanstone reference discloses the limitations of claim 1. The examiner cites Vanstone at col. 3, lines 1-7 and lines 39-43 for disclosing the limitations of step (a) of claim 1. Vanstone at col. 3, lines 1-7 reads as follows:

> i) a first of said correspondents A selecting a first random integer x and exponentiating a function $f(\alpha)$ including said generator to a power g(x) to provide a first exponentiated function $f(\alpha)^{g(x)}$;

[1] Claims 16 and 31 recite similar limitations, and thus the Applicant's remarks with respect to claim 1 apply with equally force to claims 16 and 31.

> ii) said first correspondent A generating a first signature s_A from said random integer x and said first exponentiated function $f(\alpha)^{g(x)}$; ...

Vanstone at col. 3, lines 39-43 reads as follows:

> A key 20 is associated with each of cryptographic units 16, 18 to convert plaintext carried between each unit 16, 18 and it respective correspondents 10, 12 into ciphertext carried on the channel 14.

Applicant respectfully disagrees that these passages of Vanstone disclose the limitations of step (a) of claim 1. For example, steps (i) and (ii) of Vanstone are not used to encrypt a plaintext message into a ciphertext message as required by claim 1. Instead the paragraph prior to this passage in Vanstone states that these steps (i) and (ii) are used in "a method of establishing a session key between a pair of correspondents A, B to permit exchange of information therebetween." (Vanstone, col. 2, ll. 62-64). "The session key is then used to achieve some cryptographic goal, such as privacy." (Vanstone, col. 1, ll. 29-32).

More to the point, Vanstone generates a key pair to sign a digital signature, and generates a separate session key to encrypt a plaintext message into a ciphertext message. Vanstone thus cannot anticipate "encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair" because 1) the encrypting of plaintext into ciphertext in Vanstone does not produce the claimed ephemeral key pair that is used in signing the digital signature; and 2) the establishing of the session key does not meet the claim language of "the encrypting step includes the step of producing an ephemeral key pair." (See, e.g., Vanstone, Abstract; col. 2, ln. 61 - col. 3, ln. 24; col. 4, ll. 19-36; col. 4, ln. 60 - col. 5, ln. 4; col. 5, ll. 25 - col. 6, ln. 10).

Thus, Vanstone fails to anticipate claims 1, 16, and 31. Additionally, because the rejections of all dependent claims are predicated on the incorrect rejections of claim 1, 16 and 31,

the Applicant respectfully requests that the all 35 U.S.C. §§ 102 and 103 rejections of claims 1-45 be withdrawn.

II. The IBM Reference Clearly Does Not Anticipate Claims 1, 16 And 31

The Examiner admits that the term "ephemeral key pair" is not mentioned in the IBM Reference, but concludes that the IBM Reference anticipates claims 1, 16 and 31 as it refers to the RSA algorithm:

> Note that although the phrase "ephemeral key pair" does not appear in the above mentioned passage, IBM utilizes the RSA algorithm, which is known to utilize session keys, which are by definition ephemeral keys. For example, SSL has been using these ephemeral RSA keys publicly as far back as 1993.[2]

Final Office Action, pg. 11.

This rejection is improper because it fails to show how all the limitations of claims 1, 16 and 31 are disclosed, and because the session key of the RSA algorithm is not a key pair that is used to sign a digital signature.

First, the rejection is conclusory and does not show how the IBM Reference discloses "the encrypting step includes the step of producing an ephemeral key pair." The reference does not specifically teach that an ephemeral key pair is created from an encrypting step.

The rejection also does not show how the IBM reference discloses "signing a digital signature using the ephemeral key pair." A "session key" for SSL is a symmetric key for encrypting text. It is not a key pair that is used to sign a digital signature.

---

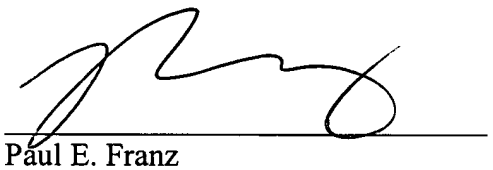
[2] The passage cited by the Examiner is not accurately quoted. Sentences are either paraphrases or quoted from several paragraphs beginning on page 1, line 39 - page 2, line 14. Additionally, this particular rejection, which is under 35 U.S.C. § 102(b), is included in the section of rejections listed under 35 U.S.C. § 103(a). However, the rejection is clearly directed to anticipation, not obviousness. Accordingly, the Applicant responds to this rejection as a 35 U.S.C. § 102(b) rejection.

Thus the IBM References has not been shown to anticipate all of the claimed limitations of claims 1, 16 or 31.

III. Conclusion

The Applicant respectfully requests the withdrawal of the rejections in light of the aforementioned arguments. It is believed that the application, as now presented, is in condition for allowance and that a Notice of Allowability be issued.

Respectfully submitted,
JONES DAY



Paul E. Franz
(Reg. No. 45,910)

Jones Day
North Point, 901 Lakeside Avenue
Cleveland, Ohio 44114
(216) 586-1162